Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

27 October 2017

PIN Number

171027-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:WHITE**: The information in this product may be distributed without restriction, subject to copyright controls.

Bad Rabbit Ransomware Targets Victims through Fake Adobe Flash Updates

Summary

Beginning on 24 October 2017, a new self-propagating ransomware variant known as Bad Rabbit began infecting media organizations in Russia and critical infrastructure in Ukraine. Bad Rabbit bears substantial resemblance to NotPetya, including shared code, shared infrastructure, very similar ransom notes, encryption of both files and the master boot record (MBR), and the ability to self-propagate. Open source reporting indicates Bad Rabbit has targeted at least 15 countries, including the United States, although the FBI is presently unaware of any successfully compromised US victims. However, the Bad Rabbit outbreak appears to be much smaller in scale, specifically targeting corporations, and has overwhelmingly impacted Russia and Ukraine.

Threat

Bad Rabbit initially infects victims via a fake Adobe Flash Player update delivered through drive-by-download on compromised websites. Users visiting compromised websites are asked to install an update to Adobe Flash, at which point a malicious download delivers the malware dropper. Upon infection, victim files are encrypted and the victim is presented with a ransom note. In all known cases, the demanded ransom has been .05 bitcoins, or roughly $280. Some private sector cybersecurity researchers speculate the actors behind Bad Rabbit may have already had a foothold in the networks of initial victims as the initial infections were reported to have occurred simultaneously.

Once installed, Bad Rabbit self-propagates across victim networks via Server Message Block (SMB) using Mimikatz, a hacking tool capable of changing privileges and recovering Windows passwords in plaintext, and a hardcoded list of commonly used default credentials to attempt to guess passwords. Furthermore, private sector analysis determined Bad Rabbit leveraged the EternalRomance exploit, one of two Shadow Broker-released exploits leveraged by NotPetya for lateral propagation. Unlike WannaCry and NotPetya, Bad Rabbit does not leverage the EternalBlue exploit.

While WannaCry and NotPetya appeared to be indiscriminate, private sector cybersecurity researchers believe Bad Rabbit is more targeted, only encrypting victims of interest based on instruction contained in the script injected into infected websites.

Recommended Steps for Prevention

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Avoid downloading any software updates unless directly from trusted sources.
- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed.

Those with a need for administrator accounts should only use them when necessary.

- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from Microsoft Office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.
- Develop, institute and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Have regular penetration tests run against the network, no less than once a year, and ideally, as often as possible/practical.
- Test your backups to ensure they work correctly upon use.

Recommended Steps for Remediation

- Contact law enforcement. We strongly encourage you to contact a local FBI field office upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.
- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so they can restore the data from a known clean backup.

Defending Against Ransomware

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.

- Only download software—especially free software—from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey